<<计算机网络安全应用教程>>

图书基本信息

书名：<<计算机网络安全应用教程>>

13位ISBN编号：9787115232960

10位ISBN编号：7115232962

出版时间：2010-9

出版时间：人民邮电出版社

作者：吴献文 编

页数：278

前言

本书是湖南省职业院校教育教学改革研究项目（项目编号：ZJGB2009013）研究成果，是国家示范性建设院校重点建设专业群内专业的建设成果，是项目驱动教学设计的实验成果。
本书是作者在总结了多年教学过程中获得的经验和心得的基础上编写的。
全书通过8个项目，按照“基本安全”、“设备安全”和“应用安全”3个层次由浅入深，由易到难地介绍了网络安全的核心技术。
通过本书的学习，读者可以快速、全面地掌握网络安全的知识与技能。
作为“项目驱动、案例教学、理论实践一体化”教学的载体，本书主要体现以下特色。
（1）组织结构新颖。
本书采用项目式写法，每个项目都设置了8个教学环节：教学导航→项目描述→项目分解→任务实施过程→知识链接→项目小结→课外拓展→课后检测，从项目准备到项目实施到效果检查，过程完整，具体的每一个任务又包括：任务布置→任务实施→任务检测→任务拓展4个环节展开，让学生明白“做什么”→“怎么做”→“做的效果”，以及让部分优秀的学生有思考、拓展的空间，解决优秀学生吃不饱的问题。
（2）项目情境真实化。
书中各个项目均依照企业项目真实实施过程来设置，体验企业真实的项目工作过程。
（3）注重实践技能培养。
本书注重培养学生动手能力，以实践为主体，理论知识遵循“必需、够用”的原则，增加学生自己动手实践比例，通过任务实施、任务拓展、任务检测层层递进；又不忽视理论的指导，以知识链接的形式补充必要的理论知识，让学生“会做，能懂”，达到知其然并知其所以然的效果。
（4）改善考核评价方式。
本书在考核评价环节作了比较大的改变，摒弃以期末考核“一槌定音”的评价方式，以项目为考核单元，整门课程的考核是一个大的项目，8个项目都各占整个项目考核的一部分，8个项目都完成后整门课程的考核也就全部完成。
另外也注意学生素质和素养的培养，将学生平时的表现也纳入考核中，以学生的综合素质培养为主。
本书由吴献文担任主编，肖耿毅、薛志良、苏岩担任副主编，陈承欢、刘志成、谢树新、林东升、李清霞、王煜煜、颜珍平、李蓓、言海燕、谭爱平、王建平等参与了部分章节的编写和文字校对工作。
由于编者水平有限，书中难免存在疏漏之处，欢迎广大读者提出宝贵的意见和建议。

<<计算机网络安全应用教程>>

内容概要

本书以“以学生为中心”的理念为指导思想，通过8个项目，按照“基本安全”、“设备安全”和“应用安全”3个层次由浅入深，由易到难地介绍了网络安全的核心技术。

主要内容包括：网络安全项目介绍与分析、操作系统安全、网络病毒与恶意软件的清除与预防、网络攻击与防范、网络监听工具应用、网络服务与应用系统安全、加密与数字签名技术的应用、防火墙与入侵检测技术的应用、无线局域网安全等网络安全技术。

全书每个项目都按照“项目描述-项目分解-任务实施-任务检查”的顺序组织教学内容，与实际工作过程相吻合，体现了完整的教学环节，强化了实践动手的技能训练，符合“学中做、做中学”的思路，适合项目驱动、理论实践一体化教学模式。

本书可作为高职高专院校计算机专业的教材，也可供计算机爱好者参考。

<<计算机网络安全应用教程>>

书籍目录

章节摘录

插图：（9）技术与管理相结合原则。
安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。
（10）易操作性原则。
首先，安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。
其次，措施的采用不能影响系统的正常运行。
步骤2：设计安全策略。
网络安全并没有绝对意义上的安全，它涉及硬件、软件、人的因素，因此没有最好，只有更好，只能尽可能地将威胁程度降低，设计一个合理可行的安全策略。
安全策略必须从用户接入终端、网络设备到中心服务器、网络设备到外网等整个网络系统安全角度考虑，而不仅是防病毒软件和防火墙的安装。
（1）物理方面。
①保护计算机系统、网络服务器、防护墙等硬件实体和通信链路不遭受自然灾害、人为破坏和搭线窃听。
②验证用户的身份和使用权限，防止用户越权操作。
③禁止非工作人员强行进入安装设备的房间，检查是否计算机系统周围存在强的磁场。
（2）访问控制方面。
访问控制是识别要访问系统的用户，控制访问权限。
包括入网访问控制、目录级安全控制、网络服务器安全控制、网络节点和端口的安全控制、防火墙访问控制等。
（3）数据加密。
明文数据很容易被识别，经过加密处理后，即使黑客获得了信息，没有密钥，得到的信息也仅仅是一堆毫无意义的乱码。
任务2-3规划网络整体安全从网络的需求来看，整个网络安全需要考虑用户安全、操作系统安全、信息传输安全、设备安全、数据库安全及计算机病毒防治等方面，因此规划网络整体安全方案需要包括网络信息保密检查、入侵检测、访问控制、病毒防范、网络管理等内容。
通过对网络结构和具体设备进行详细分析后，主要从如下几个方面采取防范措施。
（1）客户端的防护。
客户端的防护主要是保证操作系统正常运行、不受病毒的侵害和黑客的攻击，保证客户端不成为人侵网络的源头。
具体的保障措施分别在随后的项目中详细阐述。
（2）电子邮件应用广泛，而文字、声音、图像信息都可通过SMTP在网上传输，但SMTP十分简单，很不安全，因此邮件内容如果是明文，则很容易被窃听甚至被篡改，因此要加密和数字签名邮件。

编辑推荐

《计算机网络安全应用教程(项目式)》编辑推荐：是湖南省职业院校教育教学改革研究项目（项目编号：ZJGB2009013）的研究成果，是国家示范性建设院校重点建设专业群内专业的建设成果，是项目驱动教学设计的实验成果。
〈br〉《计算机网络安全应用教程(项目式)》是作者在总结多年教学经验和心得的基础上，结合企业专家的实践经验和实际工作任务来编写的。
《计算机网络安全应用教程(项目式)》以项目为导向。
结合“理论实践一体化”的教学模式。
融入完整的教学环节（每个项目都设置了8个教学环节：教学导航→项目描述→项目分解→任务实施过程→知识链接→项目小结→课外拓展→课后检测），从项目准备到项目实施到效果检查过程完整，通过任务引领，围绕“为什么要学→学什么→学了能干什么→怎么干”的思路，按照“基本安全”、“设备安全”和“应用安全”3个层次循序渐进地介绍了网络安全的核心技术，着重培养学生的职业能力和职业素质。
每一个任务都附有评价方式，让不同层次的学生都能获得成就感，激发学生的学习兴趣和学习热情。
〈br〉《计算机网络安全应用教程(项目式)》从网络安全项目介绍与分析人手，首先总体概括介绍项目情况，了解整《计算机网络安全应用教程(项目式)》的内容和结构，知道要干什么；然后具体介绍操作系统安全、网络病毒与恶意软件的清除与预防、网络攻击与防范、网络监听工具应用、网络服务与应用系统安全、加密与数字签名技术的应用、防火墙与入侵检测技术的应用、无线局域网安全等项目。
每个项目按照“项目描述、项目分解、任务卡布置任务、任务实施、任务检查”的顺序实施，与实际工作过程相吻合，设计了完整的教学环节，强化实践动手的技能训练，理论知识以需要、够用为原则进行组织，体现“学中做、做中学”。
〈br〉以项目为导向，与实际工作任务相吻合〈br〉企业任务引领，强化职业技能素质培养〈br〉教学做评一体，融合整个教学环节设计。

<<计算机网络安全应用教程>>

版权说明